EXHIBIT A

2022 WL 911207
Only the Westlaw citation is currently available.
United States District Court, D. Maryland.

PHREESIA, INC., Plaintiff,
v.
CERTIFY GLOBAL, INC., et al., Defendants.

Case No.: DLB-21-678
|
Signed 03/29/2022

Attorneys and Law Firms

Robert D. Carroll, Todd Marabella, Pro Hac Vice, Goodwin Procter LLP, Boston, MA, William Kyle Tayman, Goodwin Procter LLP, Washington, DC, for Plaintiff.

Adam Jason Lamb, Pro Hac Vice, Fox Rothschild LLP, Miami, FL, Robert P. Fletcher, Fox Rothschild LLP, Washington, DC, for Defendants.

MEMORANDUM OPINION

Deborah L. Boardman, United States District Judge

***1** Plaintiff Phreesia, Inc. ("Phreesia") filed suit against defendants Certify Global, Inc. d/b/a/ Certify and Certify Health ("Certify"), Rolling Rock Software Pvt Ltd. ("Rolling Rock"), and Timothy Goodwin, Certify's Vice President, alleging a conspiracy to misappropriate Phreesia's trade secrets, copy its software design, and interfere with its customer relationships. Phreesia claims that defendants worked with an existing Phreesia client to access Phreesia's confidential and proprietary software and incorporate the nonpublic information they acquired into their competing software system.

Phreesia asserts violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (Count I), misappropriation of trade secrets under 18 U.S.C. § 1836 *et seq.* (Count III) and Md. Code § 11-1201 *et seq.* (Count V), common law unfair competition (Count VII), and conspiracy to commit the foregoing (Counts II, IV, VI, and VIII) against all defendants. Against Certify and Goodwin, Phreesia claims tortious interference with a contractual relationship (Count IX). Against Certify and Rolling Rock, Phreesia claims unjust enrichment (Count X). Phreesia requests compensatory and punitive damages, restitution, an award of attorneys' fees and other costs, a declaration that Certify's products were unlawfully developed using Phreesia's intellectual property, and injunctive relief enjoining defendants from (i) accessing Phreesia's software, data, or information and/or (ii) incorporating any of Phreesia's information or other trade secrets into their products and services.[1]

Defendants have moved to dismiss Phreesia's amended complaint, ECF 27, for failure to state a claim. ECF 28. The motion has been fully briefed. ECF 33 & 34. A hearing is not necessary. *See* Loc. R. 105.6. For the following reasons, the motion to dismiss is granted as to Count IX and denied as to the remaining counts.

I. Background[2]

Phreesia is a Delaware corporation with its headquarters in North Carolina. ECF 27, ¶ 4. Phreesia provides point-of-service software solutions for healthcare practices nationwide through its proprietary software-as-a-service applications (the "Phreesia System"). *Id.* ¶¶ 23–24. Among other services, the Phreesia System digitizes patient intake, facilitates communication with patients, organizes patient information, automates the verification of eligibility and benefits and the calculation of copays, provides a secure payment platform, and provides data analytics. *Id.* ¶ 23. To develop its software services, Phreesia engaged in extensive research and development and product testing, investing more than $92 million over the last five years. *Id.* ¶ 25.

***2** Phreesia seeks to drive efficiency for healthcare practices while providing patients with a seamless and automated experience. *Id.* ¶ 23. To that end, the Phreesia System uses proprietary algorithms to perform complex operations—for example, where a medical practice would otherwise have to sort through potentially thousands of pages of information in different locations to determine medical billing eligibility, the Phreesia System compiles and distills the relevant information based on user queries. *Id.* ¶ 27–28. Phreesia's algorithms comprise millions of lines of code and have been carefully designed to work with the company's optimized user interfaces or "dashboards." *Id.* ¶¶ 29–31. Phreesia has established a high degree of goodwill based on the quality and utility of its software. *Id.* ¶ 26.

Phreesia regards the "code, architecture, format, structure, organization, workflows, back-end logic, functionality, operation, and interface" of its software, as well as the algorithms underlying the Phreesia System, as trade secrets. *Id.* ¶ 35. Phreesia's algorithms are stored on servers under Phreesia's control, and access requires users to sign in and agree to confidentiality provisions. *Id.* ¶¶ 32, 37–39. For example, the Phreesia "Staff Interface" can be accessed only by authorized users after a password-protected login; likewise, access to "Phreesia University" training content requires authorization and assignment to a curriculum. *Id.* ¶¶ 39–41. Phreesia logs the username, password, IP address, and date/time of each access to the Phreesia System. *Id.* ¶ 47–48. To further protect its trade secrets, Phreesia employs encryption, screens potential clients, and requires participants in its product demonstrations to sign non-disclosure agreements. *Id.* ¶¶ 36, 42–44.

Phreesia's confidentiality agreements require clients not to disclose or permit third-party access to Phreesia's software or information or use that information other than for a permitted purpose. *Id.* ¶ 36. The Phreesia System's "Master Services Agreement" provides in part:

> The receiving Party shall hold in confidence, and shall not disclose (or permit or suffer its personnel to disclose) any Confidential Information to any person or entity except to a director, officer, employee, outside consultant, or advisor (collective "Representatives") who have a need to know such Confidential Information in the course of the performance of their duties for the receiving Party and who are bound by a duty of confidentiality no less protective of the disclosing Party's Confidential Information than this Agreement. The receiving Party and its Representatives shall use such Confidential Information only for the purpose for which it was disclosed and shall not use or exploit such Confidential Information for its own benefit or the benefit of another without the prior written consent of the disclosing Party. Each Party accepts responsibility for the actions of its Representatives and shall protect the other Party's Confidential Information in the same manner as it protects its own valuable confidential information, but in no event shall less than reasonable care be used.
>
> Customer further agrees that it shall not use the products for the purposes of conducting comparative analysis, evaluations or product benchmarks with respect to the Products and will not publicly post any analysis or reviews of the Products without Phreesia's prior written approval.
>
> The Customer is responsible for (i) all activities conducted under its User logins and for its Users' compliance with this Agreement, (ii) compliance with all applicable laws and regulations that govern its business, and (iii) obtaining all authorization's [sic], consents and licenses necessary to use Customer Data. Unauthorized use, resale or commercial exploitation of the Products in any way is expressly prohibited. Without Phreesia's express prior written consent in each instance, the Customer shall not (and shall not allow any third party to): reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code form or structure of the Products or access the Products in order to build a competitive product or service or copy any ideas, features, functions or graphics of the Products. Except as expressly permitted in this Agreement, the Customer shall not copy, license, sell, transfer, make available, lease, time-share or distribute the Products to any third party.

Id. ¶ 45–46.

***3** Certify is a Delaware corporation with its headquarters in Maryland. *Id.* ¶ 5. Certify offers patient intake software services and software-as-a-service applications in competition with Phreesia. *Id.* ¶ 50–51. Rolling Rock is an Indian corporation with its U.S. headquarters in Maryland, in the same suite of the same building as Certify. *Id.* ¶ 6. Rolling Rock performs a substantial portion of Certify's software development and derives most, if not all, of its revenue from providing services to Certify. *Id.* ¶ 7. Certify and Rolling Rock are operated by the same officers and have common ownership. *Id.* ¶¶ 8–10. Defendant Goodwin is Vice President and Director of Business Development at Certify, *id.* ¶¶ 10, 59, but Phreesia does not explicitly list him among the officers common to Certify and Rolling Rock, *id.* ¶ 8.

Phreesia charges that defendants accessed the Phreesia System without authorization and, for more than a year, tested and probed the system hundreds of times with different queries to reverse engineer the underlying logic and algorithms. *Id.* ¶ 34. No defendant was ever authorized to access the Phreesia System. *Id.* ¶ 55. Instead, an existing Phreesia client created a login account for Certify in April 2018, using the name of a Certify employee, a Certify email address, and an IP address associated with Certify. *Id.* ¶¶ 56–57. Almost immediately, the account's information was changed to reflect defendant Goodwin's name and email. *Id.*

¶ 58. At some later time, the account's name was changed to "Alice Test." *Id.* ¶ 61.

Defendants used this unauthorized account "to analyze and interact with the Phreesia [S]ystem in an unauthorized manner." *Id.* ¶ 61. In 2019, the account logged in to the system more than 230 times; 130 of these login events originated from the IP address associated with Certify and Rolling Rock's Maryland headquarters, and nineteen originated from an IP address associated with Rolling Rock's offices in India. *Id.* ¶ 62–63. Through the account, defendants were able to "view the operation of the system," create and delete patient records, access Phreesia University training files, and generally "discover and reverse-engineer the functionality, structure, architecture, and workflow of the Phreesia software." *Id.* ¶ 64–65, 70–72. Goodwin and several other Certify employees used the unauthorized access to export information and send multiple emails to Certify email addresses. *Id.* ¶¶ 66–69.

Phreesia learned of Certify's unauthorized access in or around January 2021 and promptly revoked access. *Id.* ¶ 74–75. Phreesia has spent over $5,000 investigating and assessing the damage caused by the unauthorized access. *Id.* ¶ 76. It estimates the value of the information and materials disclosed without authorization exceeds $92 million. *Id.* ¶ 88. Phreesia alleges that defendants used the reverse-engineered algorithms and other information they acquired through the unauthorized account to develop and modify the user interface for Certify's competing patient management and intake software. *Id.* ¶ 77–78. As evidence, Phreesia points to a "close similarity" in the appearances of the two user interfaces, as well as many identical coding idiosyncrasies, workarounds, names and identifiers, and spelling errors. *Id.* ¶¶ 79–83. Phreesia asserts defendants' unauthorized access has resulted in a competitive advantage, allowing Certify to transition existing Phreesia customers to its systems more easily and to acquire customers it would not have but for the misappropriation of Phreesia's information. *Id.* ¶¶ 86, 89–90. For example, a major U.S. healthcare system recently selected Certify over Phreesia in a competitive process to supply software for a pilot program with the potential for future sales. *Id.* ¶ 87.

II. Standard of Review

A Rule 12(b)(6) motion to dismiss for failure to state a claim "tests the legal sufficiency of a complaint" and "should be granted unless the complaint 'states a plausible claim for relief.' " *In re Birmingham*, 846 F.3d 88, 92 (4th Cir. 2017), *as amended* (Jan. 20, 2017) (quoting *Walters v. McMahen*, 684 F.3d 435, 439 (4th Cir. 2012)); *see* Fed. R. Civ. P. 12(b)(6). To survive the motion, the "complaint need only 'give the defendant fair notice of what the ...claim is and the grounds upon which it rests.' " *Ray v. Roane*, 948 F.3d 222, 226 (4th Cir. 2020) (quoting *Tobey v. Jones*, 706 F.3d 379, 387 (4th Cir. 2013)). Stated differently, the complaint must provide "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). Importantly, a Rule 12(b)(6) motion " 'does not resolve contests surrounding the facts, the merits of a claim, or the applicability of defenses.' " *Butler v. United States*, 702 F.3d 749, 752 (4th Cir. 2012) (quoting *Edwards v. City of Goldsboro*, 178 F.3d 231, 243 (4th Cir. 1999)). In ruling on a Rule 12(b)(6) motion, the Court must accept all the plaintiff's factual allegations as true and draw all reasonable inferences in the plaintiff's favor. *In re Birmingham*, 846 F.3d at 92 (citing *E.I. du Pont de Nemours & Co. v. Kolon Indus., Inc.*, 637 F.3d 435, 440 (4th Cir. 2011)).

III. Discussion

A. "Upon information and belief" Allegations

Defendants argue Phreesia's complaint contains an "exorbitant number of allegations asserted 'upon information and belief,' " revealing the "speculative nature of its claims." ECF 28, at 24–29. Pleading upon information and belief is permissible "where the facts are peculiarly within the possession of the defendant, or where the belief is based on factual information that makes the inference of culpability plausible." *Malibu Media, LLC v. Doe*, No. PWG-13-365, 2014 WL 7188822, at *4 (D. Md. Dec. 16, 2014) (quoting *Arista Records, LLC v. Doe*, 604 F.3d 110, 120 (2d Cir. 2010)). It "is a permissible way to indicate a factual connection that a plaintiff reasonably believes is true but for which the plaintiff may need discovery to gather and confirm its evidentiary basis." *Davidson v. Sarnova, Inc.*, No. JKB-17-1067, 2017 WL 5564654, at *4 (D. Md. Nov. 20, 2017). However, pleading upon information and belief cannot save conclusory allegations; it is "an inadequate substitute for providing detail as to why the element is present in an action." *Malibu Media*, 2014 WL 7188822, at *4 (quoting *Lilley v. Wells Fargo N.A. (In re Lilley)*, No. 10-81078C-13D, 2011 WL 1428089, at *3 (Bank. M.D.N.C. Apr. 13, 2011)) (internal quotation marks omitted). In short, the federal pleading standard requires plaintiffs to identify specific facts and reasonable inferences establishing the elements of their asserted claims.

Defendants briefed their criticism of Phreesia's use of "information and belief" pleading as an independent argument. ECF 28, at 24–29. The Court will evaluate whether Phreesia has identified facts to plausibly allege its claims, keeping in mind the appropriate use of "information and belief" pleading.

B. Computer Fraud and Abuse Act (Counts I & II)

The Computer Fraud and Abuse Act ("CFAA") "is primarily a criminal statute," but "it permits private parties to bring a cause of action to redress a violation" if certain conditions are met. *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630 (4th Cir. 2009). The statute provides: "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g). A civil action may be brought only if the alleged misconduct involves, among other possibilities, "loss to 1 or more persons during any 1-year period ... aggregating at least $5,000 in value." *Id.* (referring to 18 U.S.C. § 1030(c)(4)(A)(i)(I)). Phreesia alleges defendants accessed its systems without authorization and, with intent to do so, obtained information from at least one "protected computer," causing damage in an amount of $5,000 or more in violation of 18 U.S.C. § 1030(a)(5)(A). ECF 27, ¶¶ 92–98. The CFAA defines "protected computer" as, among other things, a computer "which is used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B)

1. Access "without authorization"

Defendants argue Phreesia fails to allege defendants accessed its system "without authorization," as required by the CFAA. *See, e.g.*, 18 U.S.C. § 1030(a)(2)(C), (a)(5)(A), (a)(5)(C). The CFAA does not define "without authorization." The Fourth Circuit has interpreted the term narrowly. *Tech Sys., Inc. v. Pyles*, 630 F. App'x 184, 186 (4th Cir. 2015) (citing *WEC Carolina Energy Sols., LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012)). "[A]n employee ... accesses a computer 'without authorization' when he gains admission to a computer without approval." *WEC Carolina Energy Sols.*, 687 F.3d at 204. The definition does not "extend[ ] to the improper *use* of information validly accessed." *Id.* (emphasis in original). Additionally, the purpose or motive for accessing information is irrelevant. *Van Buren v. United States*, 141 S. Ct. 1648, 1662 (2021).

***5** Defendants argue they were authorized to access the Phreesia System by the Phreesia client pursuant to a provision in Phreesia's Master Services Agreement that excepts an "outside consultant" or "advisor" from the prohibition on the client's disclosure of "any Confidential Information to any person or entity." ECF 27, ¶ 45. Defendants argue they are outside consultants or advisors to whom the Phreesia client was permitted to disclose the Phreesia System. They reason that access as an outside consultant or advisor at the request of an authorized user forecloses liability under the CFAA. ECF 28-1, at 11–15.

Defendants cite several cases where courts have found no CFAA violation when a third party is provided with access to the computer systems at the request of an authorized user. In *SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593 (E.D. Va. 2005), the Court dismissed a CFAA claim where the plaintiff alleged an authorized user provided a competitor access to the plaintiff's confidential information on the user's servers. *Id.* at 599–601, 610. The Court reasoned that the user gave the defendants access to his server and a copy of the plaintiff's information on that server and that the defendants therefore were authorized in their access, despite the allegation that the user's conduct violated his licensing agreement with the plaintiff. *Id.* at 609–10. In *EarthCam, Inc. v. OxBlue Corp.*, 49 F. Supp. 3d 1210 (N.D. Ga. 2014), *aff'd*, 703 F. App'x 803 (11th Cir. 2017), the Court held on summary judgment that defendants who accessed the plaintiff's systems through an existing client's account with the client's permission and at the client's request did not violate the CFAA where the plaintiff had not established the client was prohibited from sharing its password with third parties. *Id.* at 1231–32. The Court distinguished *State Analysis, Inc. v. Am. Fin. Servs. Assoc.*, 621 F. Supp. 2d 309 (E.D. Va. 2009), a case that held the CFAA applied where the third-party defendant allegedly gained access by using an existing client's usernames and passwords. *EarthCam, Inc.*, 49 F. Supp. 3d at 1232. Unlike in *State Analysis*, there was no evidence that the defendants engaged in "subterfuge" to gain access, and nothing suggested they were familiar with the plaintiff's user license agreement. *Id.*; *see also* *AtPac, Inc. v. Aptitude Sols., Inc.*, No. CIV. 2:1029WBSKJM, 2010 WL 1779901, at *6 (E.D. Cal. Apr. 29, 2010) (suggesting reasoning in *State Analysis* should be limited to cases "where the third-party defendant uses subterfuge—like using user names and passwords that do not belong to it").[3]

These cases are distinguishable. *SecureInfo Corp.* concerned information stored on a private server owned by the plaintiff's client. *See* *ATPAC, Inc.*, 2010 WL 1779901, at *6 (noting the licensee in *SecureInfo Corp.* gave "the third-party access to its own servers to access the protected information"). Phreesia, by contrast, alleges it "provides access to its software services on its own secured servers," and that defendants accessed its servers remotely. ECF 2, ¶¶ 37, 62–63. *EarthCam, Inc.* is more on point, but the fully developed record in that case did not establish the client was prohibited from sharing its authorized access with the defendants. *EarthCam, Inc.*, 49 F. Supp. 3d at 1232. Phreesia, conversely, alleges just that. It claims that, notwithstanding provisions of the Master Services Agreement suggesting the Phreesia client could create an account for and authorize certain third parties access to the Phreesia System, "[n]o Defendant has ever been authorized to access the Phreesia System under the Master Services Agreement or on any other basis." ECF 27, ¶ 55. Additionally, the nature of the alleged access—hundreds of interactions that allowed defendants to reverse engineer the system's design and operating rules, followed by exporting certain information to Certify email addresses—is arguably inconsistent with the role of a consultant or advisor. *Id.* ¶¶ 62–72. From these factual allegations, it is reasonable to infer that defendants were not outside consultants or advisors to the Phreesia client within the meaning of the Master Services Agreement, that the client was prohibited from sharing its access with them, and thus, that defendants' access was indeed unauthorized.

***6** The Court will follow the reasoning in *State Analysis, Inc. v. Am. Fin. Servs. Assoc.*, 621 F. Supp. 2d 309 (E.D. Va. 2009). There, the plaintiff "pled that under the terms of their contract, only clients were authorized to use [the plaintiff's] subscription services, and that [the defendant] was not so authorized." *Id.* at 316. It did not matter that the client had provided its account information to the defendant because the client was not allowed to do so by the terms of its agreement with the plaintiff. *Id.* The Court concluded the defendant "may not hide behind purported 'authorization' granted to it" by the client, particularly because the defendant was a former client of the plaintiff and thus "presumably familiar with the terms" of the agreement. *Id.* Phreesia's allegations are analogous, even if not identical. According to Phreesia, its client was not allowed to create an account for defendants under the terms of the Master Services Agreement, which states that users "shall not ... make available ... the Products to any third party" except as "expressly permitted." ECF 27, ¶ 46. Phreesia's allegations give rise to the reasonable inference that defendants were not "outside consultants" or "advisors" or any other type of third-party user expressly permitted by the Agreement. Phreesia further alleges, upon information and belief, that defendants knew the client was bound by confidentiality provisions, "as is customary in the industry in which Phreesia and Certify both operate."[4] *Id.* ¶ 54. Even if the holding of State Analysis turned on allegations of "subterfuge," and the Court is not convinced it did, Phreesia's allegations are still analogous. Phreesia alleges defendants changed the name of the unauthorized account to "Alice Test" to "obscure their identities and involvement." *Id.* ¶ 61.

While the amended complaint is light on allegations regarding the relationship between the defendants and the Phreesia client, the Court must make all reasonable inferences in Phreesia's favor. *Ray*, 948 F.3d at 226. Because Phreesia alleges that the Master Services Agreement prohibited the Phreesia client from making the Phreesia System available to third parties except in limited circumstances that did not apply to the defendants, Phreesia has alleged defendants accessed its computer system "without authorization."

2. Statute of limitations

Defendants argue Phreesia's CFAA claim is time-barred. A defense based on the statute of limitations is an affirmative defense, and thus is generally beyond the scope of a Rule 12(b)(6) motion. However, "in the relatively rare circumstances where facts sufficient to rule on an affirmative defense are alleged in the complaint, the defense may be reached ...." *Goodman v. Praxair, Inc.*, 494 F.3d 458, 464 (4th Cir. 2007). "This principle only applies, however, if all facts necessary to the affirmative defense 'clearly appear[ ] *on the face of the complaint*.' " Id. (quoting *Richmond, Fredericksburg & Potomac R.R. v. Forst*, 4 F.3d 244, 250 (4th Cir. 1993)) (emphasis added by *Goodman*). Such is the case here.

The CFAA provides a two-year statute of limitations, running from "the date of the act complained of or the date of the discovery of the damage." 18 U.S.C. § 1030(g). Phreesia insists the relevant date for computing the limitations period is the "date of the discovery of the damage," which was in or around January 2021. *Id.* ¶ 74. If this date controls the limitations period, then the claim is timely. Defendants contend Phreesia does not allege "damage" and thus the "date of the discovery of the damage" cannot trigger the commencement of the limitations period. ECF 28-1, at 15–17. Determining the timeliness of Phreesia's CFAA claim, therefore, requires the Court to determine whether Phreesia suffered "damage" within the meaning of the statute. *See* *State Analysis, Inc.*, 621 F. Supp. 2d at 316; *Kamel v. 5Church, Inc.*, No. 3:17-CV-507-RJC-DCK, 2019 WL 4024252, at *17 (W.D.N.C. Aug. 23, 2019) (dismissing CFAA claim as time-barred where the plaintiff did not allege damage and filed its complaint more than two years after the date of the last act complained of).

The CFAA defines "damage," including as used in § 1030(g), as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Phreesia alleges defendants used their unauthorized account to log in to the Phreesia System, view its operation, access training materials, create and delete patient records, export and send information to several Certify employees, and repeatedly "test" the system to reverse engineer its architecture, algorithms, and underlying code. ECF 27, ¶¶ 62, 65, 66–71. Phreesia further alleges it has spent more than $5,000 investigating and assessing "the damage it has suffered." *Id.* ¶ 76. Defendants argue these allegations are "loss," not "damage." The statute defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, ... and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11).

***7** Phreesia responds by citing to several cases where federal courts found "damage" despite no alteration or erasure of the underlying data. *See* *SolarCity Corp. v. Pure Solar Co.*, No. CV 16-01814-BRO (DTBx), 2016 WL 11019989, at *8 (C.D. Cal. Dec. 27, 2016); *Frisco Med. Ctr., L.L.P. v. Bledsoe*, 147 F. Supp. 3d 646, 660 (E.D. Tex. 2015); *HUB Grp., Inc. v. Clancy*, No. CIV.A. 05-2046, 2006 WL 208684, at *3 (E.D. Pa. Jan. 25, 2006). Defendants counter that these cases represent the minority view. The Fourth Circuit has not addressed whether access and appropriation of confidential information, by itself, constitutes "damage" under the CFAA.

The Court is not persuaded to follow the line of cases identified by Phreesia. Each cites the same foundational case, *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000). In that case, an employee of the plaintiff sent emails to the defendant containing various trade secrets and proprietary information belonging to the plaintiff, and the plaintiff claimed CFAA violations. *Id.* at 1123. The defendant argued the plaintiff did not allege "damage" within the meaning of the statute. The Court began its analysis of "damage," defined as "any impairment to the integrity or availability of data, a program, a system, or information," by defining "integrity" as "an unimpaired or unmarred condition: entire correspondence with an original condition." *Id.* at 1126 (quoting Webster's New International Dictionary (3d ed. 1993)). Reasoning the phrase "integrity ... of data" may be ambiguous, the Court then turned to the CFAA's legislative history. It highlighted an example from the Senate Report on the 1996 amendments to the CFAA that contemplated a hacker modifying a login program to record passwords, then removing the modification from the program after retrieving the list of passwords. *Id.* at 1126. The report advised that victims of such conduct "should be entitled to relief" because the conduct "allows the intruder to accumulate valid user passwords to the system, requires all system users to change their passwords, and requires the system administrator to devote resources to resecuring the system." *Id.* (quoting S. Rep. No. 104–357, at 11 (1996)). The Court reasoned that its facts were analogous to the example in the Senate Report and concluded the collection and dissemination of confidential information, even without any change to the underlying data, constituted "damage" because it impaired the "integrity" of the data. *Id.* at 1127. It explained the impairment in the example occurred through the "accumulation of passwords and subsequent corrective measures the rightful computer owner must take to prevent the infiltration and gathering of confidential information." *Id.* at 1126–27. It did not provide a similar explanation of the impairment that occurred on the facts before it, despite no allegations that the defendant accumulated passwords or the plaintiff engaged in subsequent corrective measures. *See* *id.* at 1123 (discussing case background). Nonetheless, the Court appears to have viewed "integrity" as covering the confidentiality of information and reasoned that the collection and dissemination of confidential information can thus "impair" its integrity.

The Court is not convinced the *Shurgard* court's reliance on legislative history was appropriate where the statutory definition of "damage" has "no meaningful ambiguity." *See* *Condux Int'l, Inc. v. Haugum*, No. CIV 08-4824 ADM/JSM, 2008 WL 5244818, at *8 (D. Minn. Dec. 15, 2008) (finding "no meaningful ambiguity that might weigh in favor of relying on legislative history" to interpret "integrity" and rejecting *Shurgard's* holding) (quoting *Resdev, LLC v. Lot Builders Ass'n, Inc.*, No. 6:04-CV-1374ORL31DAB, 2005 WL 1924743, at *5 n.3 (M.D. Fla. Aug. 10, 2005)). In any event, the example from the CFAA's legislative history discussed in *Shurgard* is not analogous to these facts. Phreesia does not allege the defendants' access to and activities on the Phreesia System have resulted in either the accumulation of any other user's login information or any changes to the system necessary to "resecure" it and prevent future breaches of this nature. To the extent those consequences were also absent in *Shurgard*, that absence renders the *Shurgard* Court's holding less persuasive given the divergence between the allegations in that case and the hypothetical facts in the example cited by the Court. Indeed, "[t]he Senate Report says nothing about imposing liability ... for the taking of *information*." *See* *NetApp, Inc. v. Nimble Storage, Inc.*, No. 13-CV-05058-LHK (HRL), 2015 WL 400251, at *14 (N.D. Cal. Jan. 29, 2015) (discussing and rejecting the reasoning in *Shurgard*) (emphasis in original).

***8** The Court will instead follow the approach adopted by the apparent majority of federal courts that have held more than the copying and transmission of confidential information is required to allege "damage" under the CFAA —there must be some "diminution in the completeness or useability of data or information on a computer system." *See, e.g.*, *NetApp, Inc.*, 2015 WL 400251, at *11–15 (holding that copying confidential information and diminishing its value by making it accessible to competitors did not constitute "damage" because it did not impair the "wholeness or soundness of the information," and because no legislative history indicated "Congressional intent to impose ... liability for misappropriating information") (citing *Capitol Audio Access, Inc. v. Umemoto*, 980 F. Supp. 2d 1154, 1157–58 (E.D. Cal. 2013)); *New S. Equip. Mats, LLC v. Keener*, 989 F. Supp. 2d 522, 529–30 (S.D. Miss. 2013) (holding the copying and transmission of information did not constitute damage); *Landmark Credit Union v. Doberstein*, 746 F. Supp. 2d 990, 993–94 (E.D. Wis. 2010) (holding access and disclosure of information did not constitute damage); *Cassetica Software, Inc. v. Computer Scis. Corp.*, No. 09 C 0003, 2009 WL 1703015, at *3 (N.D. Ill. June 18, 2009) (holding "the CFAA only recognizes damage to a computer system when the violation caused a diminution in the completeness or usability of the data"); *Condux Int'l, Inc. v. Haugum*, No. CIV 08-4824 ADM/JSM, 2008 WL 5244818, at *8 (D. Minn. Dec. 15, 2008) (stating "the complained of activity must have an effect on the binary coding used to create, store, and access computerized representations of information" and holding the downloading and disclosure of confidential information did not constitute damage); *Lockheed Martin Corp. v. Speed*, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *8 (M.D. Fla. Aug. 1, 2006) (holding the alleged wrongful taking of trade secrets does not constitute damage) (citing *Resdev, LLC v. Lot Builders Ass'n, Inc.*, No. 6:04-CV-1374ORL31DAB, 2005 WL 1924743, at *4 (M.D. Fla. Aug. 10, 2005)).

These courts used rules of statutory interpretation to read "damage" narrowly. The courts defined "integrity" as concerning "wholeness" or "soundness" and reasoned, as used in the CFAA, the term concerns the "diminution in the completeness or usability of the data on a computer system." *See* *NetApp, Inc.*, 2015 WL 400251, at *12 (identifying common definition in precedent); *Cassetica Software, Inc.*, 2009 WL 1703015, at *3 (same definition). With integrity defined as "wholeness" or "soundness," the term "damage" includes, for example, "the destruction, corruption, or deletion of electronic files," as well as "the physical destruction of a hard drive." *Farmers Ins. Exch. v. Auto Club Grp.*, 823 F. Supp. 2d 847, 852 (N.D. Ill. 2011). It does not cover "the disclosure to a competitor of its trade secrets and other confidential information." *Id.* (paraphrasing *Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760, 769 (N.D. Ill. 2009)); *see also* *NetApp, Inc.*, 2015 WL 400251, at *12. This approach is logically coherent, easy to apply, and faithful to the statutory text. Moreover, it is consistent with what limited guidance is available from the Fourth Circuit on the scope of the CFAA. *See* *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 203 (4th Cir. 2012) (agreeing with *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (en banc), which warned against interpreting the CFAA broadly as "an expansive misappropriation statute," in the context of interpreting "without authorization").

Phreesia does not allege defendants affected the "wholeness" or "soundness" of its data or information or that the defendants caused "any diminution in the completeness or usability of the data." The Phreesia System was no less whole, sound, complete, or usable after defendants accessed it. And unlike the example discussed in *Shurgard*, Phreesia does not allege any collection of user credentials or other conduct that might require steps to resecure the system. Rather, Phreesia alleges only the unauthorized access, copying, exporting, and misuse of data and information.[5] These allegations do not constitute an impairment of the integrity of its data and information. Phreesia therefore does not allege it suffered "damage" within the meaning of 18 U.S.C. § 1030(e)(8).

***9** Because Phreesia does not allege "damage," it follows that Phreesia did not discover "damage," and the two-year limitations period for Phreesia's CFAA claim began to run from "the date of the act complained of." 18 U.S.C. § 1030(g). The parties agree that the date of the first act complained of is April 18, 2018, when defendants allegedly first gained access to the Phreesia System through an unauthorized account. ECF 27, ¶ 56.

Defendants argue that if April 18, 2018 marks the running of the limitations period, the two-year period would have lapsed on April 18, 2020, and the CFAA claim would be time-barred because Phreesia did not file suit until March 17, 2021. This argument ignores Phreesia's allegation that defendants continued to access the system hundreds of times over the course of 2019. *Id.* ¶ 62. At most, defendants' argument would narrow the claim to misconduct that occurred before March 17, 2019, two years before the complaint was filed. This separate-accrual approach to computing the limitations period is appropriate where "the law forbids a discrete act, as most do ...." *Blake v. JP Morgan Chase Bank NA*, 927 F.3d 701 (3d Cir. 2019); *see also* *Petrella v. Metro-Goldwyn-Mayer, Inc.*, 572 U.S. 663, 671 (2014) (applying separate-accrual rule in copyright context); *Coakley & Williams, Inc. v. Shatterproof Glass Corp.*, 706 F.2d 456, 463 (4th Cir. 1983) (allowing otherwise time-barred claim to proceed because subsequent conduct "constituted a distinct and separate accrual for purposes of computing the limitations period"). Other courts have applied the separate-accrual rule to claims under the CFAA. *See* *State Analysis, Inc. v. Am. Fin. Servs. Assoc.*, 621 F. Supp. 2d 309, 316 (E.D. Va. 2009) (dismissing parts of CFAA claim relating to violations that occurred more than two years before the complaint was filed where the plaintiff did not allege damage); *In re Dealer Mgmt. Sys. Antitrust Litig.*, No. 18-CV-864, 2019 WL 4166864, at *8–9 (N.D. Ill. Sept. 3, 2019) (dismissing parts of CFAA claim based on violations more than two years before the plaintiff filed suit); *Sewell v. Bernardin*, 795 F.3d 337, 340–41 (2d Cir. 2015) (dismissing part of CFAA claim discovered outside the limitations period); *but see* *Meyer Tech. Sols., LLC v. Kaegem Corp.*, 2017 WL 4512918, at *1 (N.D. Ill. Oct. 10, 2017) (dismissing entire CFAA claim as time-barred despite the allegation that the party "may have continued accessing certain parts of [the] business information housed on the [ ] platform in the same fashion" within the limitations period).

Continuing or continuous violations—multiple, discrete acts that accrue separately—are distinct from a cumulative violation, where multiple acts are necessary to create one violation. *See* *Blake*, 927 F.3d at 706 (explaining distinction); *Limestone Dev. Corp. v. Vill. of Lemont, Ill.*, 520 F.3d 797, 801–02 (7th Cir. 2008) (same). In cases involving the latter, the limitations period may be tolled to cover the entire course of conduct because if each act "had to be considered in isolation, there would be no claim even when by virtue of the cumulative effect of the acts it was plain that the plaintiff had suffered actionable" injury. *Limestone Dev. Corp.*, 520 F.3d at 801; *see also* *Nat'l R.R. Passenger Corp. v. Morgan*, 536 U.S. 101 (2002) (adopting cumulative violation approach in workplace discrimination context). Other courts have considered the cumulative violation approach in the CFAA context, but no court has adopted it. *See* *Radcliff v. Radcliff*, No. CV 20-3669, 2020 WL 7090687 (D.N.J. Dec. 4, 2020) (considering argument that cumulative approach applied in CFAA context but declining to rule on that point and dismissing because the plaintiff failed to allege any violation occurred within the limitations period); *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 137–38 (N.D. Cal. Apr. 7, 2020) (holding "continuing" violation doctrine, which other courts would call cumulative, could not save a CFAA claim where the conduct complained of was a single discrete event that occurred outside the limitations period); *In re Dealer Mgmt. Sys. Antitrust Litig.*, 2019 WL 4166864, at *8–9 (declining to apply cumulative approach where the party did not identify any facts indicating its CFAA counterclaim was based on "the cumulative effect of a series of acts"); *Meyer Tech. Sols., LLC*, 2017 WL 4512918, at *1 (declining to apply cumulative approach in the CFAA context because the plaintiff had not alleged facts showing "the 'cumulative effect' of a series of acts" was necessary to make out an actionable CFAA claim). Neither party addressed the distinction between continuous and cumulative violations or its effect on the computation of the limitations period here. Consistent with these cases and in the absence of contrary argument, the Court will follow the separate-accrual approach to computing the limitations period.

***10** Under the separate-accrual approach, Phreesia's CFAA claim is timely to extent it is based on acts of unauthorized access that occurred within two years of the date Phreesia filed suit. Thus, to the extent the claim is based on misconduct occurring before March 17, 2019, it is time-barred. *See* *State Analysis, Inc.*, 621 F. Supp. 2d at 316; *In re Dealer Mgmt. Sys. Antitrust Litig.*, 2019 WL 4166864 at *8–9. Phreesia alleges defendants logged in to its system "more than 230 times during 2019." ECF 27, ¶ 62. It is reasonable to infer that some number of these logins occurred within the limitations period. Because the Court is satisfied that Phreesia alleges a potential CFAA violation occurring within the limitations period, the motion to dismiss is denied as to Count I. [6]

3. Conspiracy to violate the CFAA

The Court's rulings on the CFAA claim apply to the related conspiracy claim. Civil conspiracy is "the 'combination of two or more persons by an agreement or understanding to accomplish an unlawful act or to use unlawful means to accomplish an act not in itself illegal, with the further requirement that the act or the means employed must result in damages to the plaintiff.' " *Marshall v. James B. Nutter & Co.*, 758 F.3d 537, 541 (4th Cir. 2014) (quoting *Hoffman v. Stamper*, 867 A.2d 276, 290 (Md. 2005)). The Fourth Circuit and the Maryland Court of Appeals have held that a plaintiff cannot prevail on a claim for civil conspiracy under Maryland law "in the absence of other tortious injury to the plaintiff." *Id.* at 541 (quoting *Alleco Inc. v. Harry & Jeanette Weinberg Found., Inc.*, 665 A.2d 1038, 1045 (Md. 1995)); *see also* *Arkansas Nursing Home Acquisition, LLC v. CFG Cmty. Bank*, 460 F. Supp. 3d 621, 647 (D. Md. 2020) ("Under Maryland law, there is no separate tort for civil conspiracy; instead, a civil conspiracy theory merely serves to extend liability to the co-conspirators after some other tortious conduct is established.").

Here, the underlying tortious conduct is the CFAA violation. Phreesia has alleged a CFAA violation, and thus it also has alleged a conspiracy to violate that statute. The motion to dismiss is denied as to Count II. Where the other alleged torts underlying Phreesia's conspiracy claims survive dismissal, the related conspiracy claims also survive.

C. Misappropriation of trade secrets (Counts III, IV, V, & VI)

To state claim for misappropriation of trade secrets under The Defense Trade Secrets Act ("DTSA") and its Maryland equivalent, the Maryland Uniform Trade Secrets Act ("MUTSA"), a plaintiff must allege "that the documents at issue are trade secrets and that the defendant misappropriated those trade secrets." *Philips N. Am. LLC v. Hayes*, No. ELH-20-1409, 2020 WL 5407796, at *7 (D. Md. Sept. 9, 2020). Specifically, the DTSA requires the plaintiff to allege "(1) it owns a trade secret which was subject to reasonable measures of secrecy; (2) the trade secret was misappropriated by improper means; and (3) the trade secret implicates interstate or foreign commerce." *Id.* (citing 18 U.S.C. § 1836(b)(1)). The MUTSA requires the plaintiff to establish that "(1) it possessed a valid trade secret, (2) the defendant acquired its trade secret, and (3) the defendant knew or should have known that the trade secret was acquired by improper means." *Id.* (quoting *Trandes Corp. v. Guy F. Atkinson Co.*, 996 F.2d 655, 660 (4th Cir. 1993)).

1. Existence of trade secrets

Defendants argue Phreesia fails to identify any potential trade secrets. The DTSA and the MUTSA define "trade secret" in a similar manner. *Id.* at *8. A "trade secret" includes all forms of information, including economic and engineering information, "if (1) the owner has taken reasonable measures to keep such information secret; and (2) the information derives independent economic value, actual or potential, from not being generally known to another person in the relevant industry, and not being readily ascertainable through proper means." *Id.* (citing 18 U.S.C. § 1839(3) and Md. Code, Commercial Law, § 11-1201(e)).

Phreesia's amended complaint alleges each element of a trade secret under the DTSA and MUTSA. As an initial matter, Phreesia alleges information within the class covered by the statutes: "the software code, architecture, format, structure, organization, workflows, back-end logic, functionality, operation, and interface of the Phreesia System," as well as the "underlying algorithms, including the proprietary Phreesia eligibility and payment algorithms[.]" ECF 27, ¶¶ 35, 111–12. Phreesia's software streamlines the process of sorting the "mountain of information" available across "thousands of pages ... from many private and government insurers, medical practices and providers, and billing systems across the country" and compiling "clear and usable responses." *Id.* ¶¶ 27–28. Each algorithm represents "potentially thousands of possible logic tree pathways." *Id.* ¶ 33. The algorithms "work hand-in-hand" with Phreesia's user interfaces, which were specially developed, at substantial investment, "to ensure that users enter the right information to distill out the data they need." *Id.* ¶ 31.

Defendants challenge whether these allegations describe the alleged trade secrets with enough detail. ECF 28-1, at 17. They point to other federal district court cases that held, under the DTSA, a plaintiff must "identify a trade secret with sufficient particularity so as to provide notice to a defendant of what he is accused of misappropriating and for a court to determine whether misappropriation has or is threatened to occur." *Lithero, LLC v. AstraZeneca Pharms. LP*, No. 19-2320-RGA, 2020 WL 4699041, at *1–2 (D. Del. Aug. 13, 2020)); *see also, e.g.*, *Vendavo, Inc. v. Price f(x) AG*, No. 17-CV-06930-RS, 2018 WL 1456697, at *4 (N.D. Cal. Mar. 23, 2018) (dismissing DTSA claim where the plaintiff "set out its purported trade secrets in broad, categorical terms, more descriptive of the types of information that generally may qualify as protectable trade secrets than as any listing of particular trade secrets [it] has a basis to believe actually were misappropriated here"); *AlterG, Inc. v. Boost Treadmills LLC*, 388 F. Supp. 3d 1133, 1144 (N.D. Cal. 2019) (dismissing claim for reasons similar to *Vendavo*). Relying on these cases, defendants argue Phreesia alleges only "large, general areas of information," rather than particularized trade secrets. *See* ECF 28-1, at 19.

Phreesia does not dispute that the "sufficient particularity" requirement applies at the motion to dismiss stage in this jurisdiction, though it offers a different formulation of the rule. ECF 33, at 15 (quoting *Albert's Organics, Inc. v. Holzman*, 445 F. Supp. 3d 463, 472 (N.D. Cal. 2020) (stating the plaintiff must "describe the subject matter of the trade secret with sufficient particularity to separate it from matters of general knowledge in the trade or of special persons who are skilled in the trade, and to permit the defendant to ascertain at least the boundaries in which the secret lies")). The only cases the parties cite from this jurisdiction do not use similar language. *See* *Philips N. Am. LLC*, 2020 WL 5407796, at *8 (discussing what constitutes a trade secret without mentioning any required degree of particularity or specificity); *Bindagraphics, Inc. v. Fox Grp., Inc.*, 377 F. Supp. 3d 565, 577 (D. Md. 2019) (stating only "the complaint is not clear enough as to what Bindagraphics trade secret [the defendant] is alleged to have taken"). The clearest Fourth Circuit guidance states, at the summary judgment stage, that the plaintiff must "describe the subject matter of its alleged trade secrets in sufficient detail to establish each element of a trade secret." *Trandes Corp. v. Guy F. Atkinson Co.*, 996 F.2d 655, 661 (4th Cir. 1993) (citations omitted). Other courts in this district have previously applied some form of a "sufficient particularity" requirement before commencing discovery, *see* *Structural Pres. Sys., LLC v. Andrews*, No. 12-1850-MJG, 2013 WL 12244886, at *3 (D. Md. Dec. 17, 2013); during discovery, *see* *Hempel v. Cydan Dev.*, No. PX-18-3404, 2020 WL 8167432, at *1 (D. Md. June 3, 2020); and at the summary judgment stage, *see* *Albert S. Smyth Co. v. Motes*, No. CCB-17-677, 2020 WL 4471524, at *3 (D. Md. Aug. 3, 2020).

***12** Whether or not the "sufficient particularity" standard applies, Phreesia's allegations survive a motion to dismiss. Phreesia paints a reasonably detailed picture of the alleged trade secrets at issue—the unique ways Phreesia has designed its software and user interfaces to streamline operations, sort and categorize information, nudge users, and provide only the information that is required by any given user query. ECF 27, ¶¶ 27–35, 111–12. Moreover, Phreesia alleges defendants incorporated its trade secrets into their competing product, noting a "close similarity between the Certify user interface and Phreesia's proprietary interface" and the presence of "the same coding idiosyncrasies and workarounds for features unique to the Phreesia System." *Id.* ¶¶ 79–84. "A side-by-side comparison" allegedly shows the interfaces "are almost identical in look and function." *Id.* ¶ 79. These allegations provide notice to defendants of what they are "accused of misappropriating," and, if supported by evidence, will allow the Court "to determine whether misappropriation has or is threatened to occur." *Lithero, LLC*, 2020 WL 4699041, at *1–

2. Put another way, the allegations permit the defendants "to ascertain at least the boundaries in which" the alleged secrets lie. *Albert's Organics, Inc.*, 445 F. Supp. 3d at 472.

Having sufficiently alleged the type of information covered by the DTSA and MUTSA, Phreesia must allege that it has taken reasonable measures to keep this information secret. It has. Phreesia required its clients to sign confidentiality agreements, and it used remote servers and controlled access to the Phreesia System via encryption and password protection. ECF 27, ¶¶ 32, 36–49. Defendants do not raise any arguments to the contrary.

Finally, Phreesia must allege that its proprietary software and algorithms derive independent economic value from not being generally known in its industry or readily ascertainable through proper means. It has done so. Phreesia alleges its algorithms are not publicly disclosed or available. *Id.* ¶ 32. Each algorithm "represents potentially thousands of possible logic tree pathways," so users "will likely only experience a small amount of the functionality" of any algorithm. *Id.* ¶ 33. In other words, the algorithms are not "known" even to Phreesia's users. To "reverse engineer and derive the underlying logic" of the algorithms, it would take "hundreds of logins" to chart the software's responses to different queries. *Id.* ¶ 34. Finally, the cost of developing Phreesia's algorithms and the security measures it has implemented to protect them imply value worth protecting—the value of not being generally known. *Id.* ¶¶ 25, 36–49.

Defendants argue it is not clear from the complaint why Phreesia's algorithms would derive value from their confidentiality, as the patient intake process is "a well-established practice at doctors' offices" and "methods for mechanical collection of patient information" should be readily ascertainable and generally known to others in the industry. ECF 28-1, at 19–20. Defendants cite *WeInfuse, LLC v. InfuseFlow, LLC*, No. 3:20-CV-1050-L, 2021 WL 1165132 (N.D. Tex. Mar. 26, 2021) for the proposition that patient intake software similar to Phreesia's is not a protectable trade secret. In that case, the plaintiff alleged the misappropriation of its trade secrets, consisting of "every aspect of the Software architecture behind the protected login." *Id.* at *3. The plaintiff offered only a list of "features and functionalities" on its user interface. *Id.* The Court dismissed the DTSA claims because the alleged "descriptions and offerings are far too broad to qualify as trade secrets." *Id.* The plaintiff "failed to point to specificities that convey the unique capabilities of the Software," so the Court could not reasonably infer "that the Software's features and functionalities ... are not generally known within the industry or readily ascertainable through proper means." *Id.* (citing *GlobeRanger Corp. v. Software AG United States of Am., Inc.*, 836 F.3d 477, 492 (5th Cir. 2016)).

Defendants' argument mischaracterizes Phreesia's allegations, which describe the way Phreesia collects, sorts, and displays information as complex and proprietary rather than mechanical and readily ascertainable within the industry. Phreesia identifies measures it takes to keep this technical information secret. ECF 27, ¶¶ 32, 36–48. While the alleged software at issue in *WeInfuse* appears to be similar to the software at issue here, the case is nonetheless distinguishable. In contrast to the plaintiff's allegations in *WeInfuse*, Phreesia alleges that its algorithms are uniquely capable of performing the complex operations described above, and it provides more detail than a list of elements found in its user interfaces. Moreover, Phreesia alleges its algorithms are the result of "thousands of hours and millions of dollars," are composed of "millions of lines of code," and are constantly improved through "state-of-the-art machine learning." *Id.* ¶ 29. It can be reasonably inferred from these allegations that the information Phreesia describes is not generally known in the industry or readily ascertainable through proper means. Rather, it could be obtained only by "repeatedly entering queries with slightly differing information over the course of hundreds of logins and charting the software's responses," *id.* ¶ 34, as defendants are alleged to have done, *id.* ¶¶ 34, 62–65.

***13** Phreesia thus alleges the misappropriation of trade secrets. The motion to dismiss is denied as to Counts V and VI.

2. Use in interstate commerce

To state a claim under the DTSA, plaintiffs must allege that "the trade secret implicates interstate or foreign commerce." *Philips N. Am. LLC*, 2020 WL 5407796, at *7–8. Defendants argue Phreesia has not alleged that its trade secrets are related to a product or service used in, or intended for use in, interstate or foreign commerce. They focus on the Phreesia client, *see* ECF 27, ¶ 53, whom they claim is a Maryland-based physician's office, ECF 28-1, at 22. This fact was not alleged in the amended complaint. In any event, this argument has no merit. Phreesia is a Delaware corporation with its headquarters in North Carolina. *Id.* ¶ 4. Its servers are in North Carolina, and it offers access to its products over the internet. *Id.* ¶¶ 4, 32, 37. It is engaged "in the nationwide business of providing point-of-service software solutions for healthcare practices ...." *Id.* ¶ 23. Thus, Phreesia has alleged that its trade secrets implicate and are used in interstate commerce. *See* *Philips N. Am. LLC*, 2020 WL 5407796, at *11 (holding complaint alleged use in interstate commerce where the plaintiff alleged its business "is both national and international") (citing *Albert S. Smyth Co., Inc.*, 2018 WL 3635024, at *3).

Accordingly, the motion to dismiss is denied as to Counts III and IV.

D. Unfair competition (Counts VII & VIII)

Under Maryland law, "[u]nfair competition is 'damaging or jeopardizing another's business by fraud, deceit, trickery or unfair methods of any sort.' " *Elecs. Store, Inc. v. Cellco P'ship*, 732 A.2d 980, 991 (Md. Ct. Spec. App. 1999) (quoting *Balt.* *Bedding Corp. v. Moses*, 34 A.2d 338, 342 (Md. 1943)); *Farm Fresh Direct Direct By a Cut Above LLC v. Downey*, No. ELH-17-1760, 2017 WL 4865481, at *10 (D. Md. Oct. 26, 2017); *see also* *Thompson v. UBS Financial Services, Inc.*, 115 A.3d 125, 133 (Md. 2015) (reaffirming the rule). "[T]he Maryland Court of Appeals 'has preserved a high degree of flexibility in the law of unfair competition.' " *Farm Fresh Direct*, 2017 WL 4865481, at *10 (citing *Delmarva Sash & Door Co. of Md., Inc. v. Andersen Windows, Inc.*, 218 F.Supp.2d 729, 733 (D. Md. 2002)).

> What constitutes unfair competition in a given case is governed by its own particular facts and circumstances. Each case is a law unto itself, subject, only, to the general principle that all dealings must be done on the basis of common honesty and fairness, without taint of fraud or deception.

Id. (quoting *Balt.* *Bedding*, 34 A.2d at 342). However, "only acts which 'substantially interfere[ ] with the ability of others to compete on the merits of their products' or acts that 'conflict[ ] with accepted principles of public policy' can serve as the grounds of an unfair competition claim." *Ellicott Dredges, LLC v. DSC Dredge, LLC*, 280 F. Supp. 3d 724, 732 (D. Md. 2017) (quoting *Sprint Nextel Corp. v. Simple Cell Inc.*, 248 F. Supp. 3d 663, 687 (D. Md. 2017), *vacated and remanded sub nom. on other grounds*, *Sprint Nextel Corp. v. Wireless Buybacks Holdings, LLC*, 938 F.3d 113 (4th Cir. 2019)).

***14** Defendants argue that the unfair competition and related conspiracy claims are premised on the trade secrets claims and must fall if those claims are dismissed. Because Phreesia's trade secrets claims survive, this argument fails.

Defendants next challenge the adequacy of the alleged harm. Phreesia alleges that, as a result of the defendants' unfair competition, it lost to Certify a recent bid for a contract with a major U.S. healthcare network. ECF 27, ¶ 87. Defendants argue this alleged harm is speculative. They claim the bidding process involved other companies and Certify's selection could have been the result of other factors, such as "price, terms, scope of services, reputation, other services provided by the company, management, etc." ECF 28-1, at 23. Thus, defendants argue, even if Certify had not had the competitive advantage from its alleged incorporation of Phreesia's confidential information into its own product, there is no guarantee that the customer would have selected Phreesia for the contract.

These arguments are unconvincing. First, they are premised on facts not alleged in the amended complaint. The Court's review is limited to the complaint's allegations, and Phreesia alleges that the event was "a competitive process" that involved the two companies, with no mention of other companies. The Court does not resolve factual disputes on a motion to dismiss. *Butler*, 702 F.3d at 752. Second, that Certify's selection over Phreesia could have been the result of factors beyond the alleged wrongful competitive advantage does not make it implausible that the competitive advantage played a role. The Court must make all reasonable inferences in favor of the plaintiff. *In re Birmingham*, 846 F.3d at 92. Finally, Phreesia alleges this event is "just one example" of Certify using its wrongful competitive advantage to gain "customers" "that [it] would not have but for Defendants' wrongful acts." ECF 27, ¶¶ 86–87.

Phreesia plausibly alleges unfair competition under Maryland law. Accordingly, the motion to dismiss is denied as to Count VII and Count VIII.

E. Tortious interference with a contractual relationship (Count IX)

"To establish a claim for wrongful interference with a contract, a plaintiff must demonstrate '(1) [t]he existence of a contract or a legally protected interest between the plaintiff and a third party; (2) the defendant's knowledge of the contract; (3) the defendant's intentional inducement of the third party to breach or otherwise render impossible the performance of the contract; (4) without justification on the part of the defendant; (5) the subsequent breach by the third party; and (6) damages to the plaintiff resulting therefrom.' " *Painter's Mill Grille, LLC v. Brown*, 716 F.3d 342, 353–54 (4th Cir. 2013) (quoting *Blondell v. Littlepage*, 968 A.2d 678, 696 (Md. 2009)).

Defendants argue that Phreesia's allegations about the defendants' knowledge of the Master Services Agreement and their intentional inducement of a breach are based upon information and belief and lack the factual support required to plausibly state a claim of tortious interference. ECF 34, at 21–22. The Court agrees that Phreesia has not plausibly alleged intentional inducement to breach. The following distinction between allegations illuminates the problem well. Regarding knowledge of the agreement, Phreesia alleges on information and belief that similar provisions "prohibiting disclosure, unauthorized access and reverse engineering" are "customary in the industry in which Phreesia and Certify both participate." ECF 27, ¶ 54. The existence of an industry custom is a specific factual allegation, and from that allegation, the Court can infer defendants' knowledge that the industry client was bound by customary confidentiality provisions. Conversely, regarding defendants' intent to induce a breach, Phreesia alleges on information and belief that defendants "knowingly induced" breach and "conspired" with the client to breach the agreement. *Id.* ¶ 53–54. These are not factual allegations from which the Court can infer defendants' intent to induce breach, but rather a statement of the legal element at issue. Phreesia does not allege any facts about the relationship between Certify and the Phreesia client from which the Court could infer how Certify may have induced the breach, such as who approached whom regarding the allegedly unauthorized account or what motivated the client to create and share the account.

***15** This case is similar to *Painter's Mill Grille, LLC v. Brown*, 716 F.3d 342 (4th Cir. 2013). In that case, the plaintiff operated a restaurant on premises leased to it by the one of the defendants. *Id.* at 345. Two other defendants were common employees of the two companies. *Id.* The plaintiff alleged that the two employee defendants interfered with a contract to sell the plaintiff's interest in the restaurant by making racist and derogatory comments about the plaintiff and its clientele at a meeting about the sale. *Id.* at 346. Plaintiff further alleged it entered into a subsequent contract to sell the restaurant, and the defendants again induced the third party to breach the contract. *Id.* at 354. The Fourth Circuit affirmed dismissal of the first tortious interference claim because the plaintiff's allegations "regarding *how* the defendants intentionally interfered with this contract fail to state a claim that is facially plausible." *Id.* (emphasis in original). While the complaint alleged the individual defendants made derogatory comments at a meeting with the buyer, it lacked detail regarding what was said and made only a "bare assertion that the statements were made with the requisite intent." *Id.* Regarding the second tortious interference claim, the panel concluded it stood on even weaker ground because the plaintiff did not provide "*any* factual allegations regarding how the defendants effected" the alleged interference. *Id.* (emphasis in original). The panel found the second claim "supported by nothing more than 'a formulaic recitation of the elements of [the] cause of action' it purports to assert," and affirmed dismissal. *Id.* (citing *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)).

Like the plaintiff in *Painter's Mill Grille*, Phreesia has not plausibly alleged tortious interference under Maryland law. Its allegations regarding defendants' intentional inducement of the Phreesia client to breach the Master Services Agreement recite the element at issue and are otherwise devoid of specific factual content. *See Service 1st Vending, Inc. v. Compass Grp. USA, Inc.*, DKC-20-3723, 2021 WL 1312906, at *3 (D. Md. Ap. 8, 2021) (dismissing tortious interference claim where "the nature of the supposed interference is unclear" and the plaintiff did not allege facts allowing an inference of the requisite intent); *Jennings v. Hous. Auth. of Balt. City*, No. WDQ-13-2164, 2014 WL 346641, at *8 (D. Md. Jan. 29, 2014) (dismissing tortious interference claim where the plaintiff did not allege "any facts that would allow the Court to infer that the [defendant's conduct] caused the destruction of her business relationship"); *cf. Webb v. Green Tree Servicing, LLC*, No. ELH-11-2105, 2011 WL 6141464, at *7 (D. Md. Dec. 9, 2011) (holding tortious interference claim survived dismissal where the complaint alleged "ample facts" about the defendant's alleged conduct inducing the breach, allowing an inference of the requisite intent).

Accordingly, the motion to dismiss is granted as to Count IX, and the tortious interference claim is dismissed.

F. Unjust enrichment (Count X)

Unjust enrichment requires proof of three elements: "(1) A benefit conferred upon the defendant by the plaintiff; (2) An appreciation or knowledge by the defendant of the benefit; and (3) The acceptance or retention by the defendant of the benefit under such circumstances as to make it inequitable for the defendant to retain the benefit without payment of its value." *Hill v. Cross Country Settlements, LLC*, 936 A.2d 343, 351 (Md. 2007) (quoting *Berry & Gould, P.A. v. Berry*, 757 A.2d 108, 113 (Md. 2000)).

Defendants argue that a claim for unjust enrichment cannot stand alone and must be dismissed absent an underlying tort claim. ECF 28-1, at 30. The case defendants cite for this proposition expressly noted that Maryland law appeared to be unsettled on the issue. *Washington Cty. Bd. of Educ. V. Mallinckrodt ARD, Inc.*, 431 F. Supp. 3d 698, 718 (D. Md. 2020) ("It is not clear to the Court whether it is permissible under Maryland law for a suit to consist of a single claim for unjust enrichment without an accompanying underlying tort."). The Court nonetheless erred against "overstep[ping] its bounds" and decided to dismiss the claim "without more clearly supportive precedent." *Id.* Because several of Phreesia's other claims survive the motion to dismiss, this Court need not decide whether a claim of unjust enrichment can survive without a host tort under Maryland law. Several are present, if necessary.

Defendants alternatively argue that Phreesia has failed to plead the specific benefit conferred or the defendants' appreciation of the benefit. ECF 28-1, at 30–31; ECF 34, at 23–24. The Court disagrees. Phreesia has alleged that defendants, through their unauthorized access of the Phreesia System, acquired confidential information, trade secrets, and reverse-engineered algorithms, ECF 27, ¶¶ 34–35, 62–65, 70–72; that defendants incorporated this information into their own systems and user interface, *id.* ¶¶ 77–84; and that as a result, defendants have gained a competitive advantage, including the ability to more easily transition existing Phreesia clients to Certify's systems and the award of a specific contract from a major national healthcare system, *id.* ¶¶ 86–90. Information is a benefit, and Phreesia estimates this collection of information is worth $92 million. *Id.* ¶¶ 29, 88. Assuming Phreesia's allegations are true, it is reasonable to infer defendants appreciated that benefit because they used it to improve their competing product.

***16** Because Phreesia alleges unjust enrichment, the motion to dismiss is denied as to Count X.

G. Scope of dismissal

Defendants request dismissal with prejudice, arguing that Phreesia already had an opportunity to amend its complaint. ECF 28-1, at 31. Phreesia requests any dismissal be without prejudice and with leave to amend under Rule 15(a)(2). ECF 33, at 28. The decision whether to grant leave to amend "is within the sound discretion of the district court, but 'the federal rules strongly favor granting leave.' " *Hinks v. Bd. of Educ. of Hartford Cnty.*, No. WDQ-09-1672, 2010 WL 5087598, at *2 (D. Md. Dec. 7, 2010) (quoting *Medigen of Kentucky, Inc. v. Pub. Serv. Comm'n of W. Virginia*, 985 F.2d 164, 167–68 (4th Cir. 1993)).

> In the absence of any apparent or declared reason—such as undue delay, bad faith or dilatory motive on the part of the movant, repeated failure to cure deficiencies by amendments previously allowed, undue prejudice to the opposing party by virtue of allowance of the amendment, futility of amendment, etc.—the leave sought should, as the rules require, be "freely given."

Foman v. Davis, 371 U.S. 178, 182 (1962).

Phreesia will not be granted leave to amend Count I, the CFAA claim. The Court's ruling narrowing the CFAA claim is based on Phreesia's failure to allege "damage" under the statute. Given the nature of the misconduct Phreesia alleges and the narrow definition of "damage" under the CFAA, amendment would be futile on this issue. *See United States ex rel. Carson v. Manor Care, Inc.*, 851 F.3d 293, 305 (4th Cir. 2017) ("[W]hen a complaint is incurable through amendment, dismissal is properly rendered with prejudice and without leave to amend.”) (citing *McLean v. United States*, 566 F.3d 391, 400 (4th Cir. 2009), *abrogated on other grounds by Lomax v. Ortiz-Marquez*, 140 S. Ct. 1721 (2020)).

Count IX, tortious interference, is dismissed without prejudice. Dismissal of this claim is warranted because Phreesia did not allege specific facts capable of supporting the reasonable inference that defendants induced the Phreesia client to violate the Master Services Agreement. While defendants did raise this specific deficiency in their notice of intent to file a motion to dismiss, id. at 3, “the Court is cognizant that discovery could unearth additional facts that would permit” Phreesia to amend its complaint to allege inducement, *see Doe v. Johns Hopkins Health System Corporation*, 274 F. Supp. 3d 355, 369 (D. Md. 2017) (dismissing claim without prejudice where it lacked necessary factual allegations that were also outside the plaintiff's knowledge). Details surrounding the relationship between defendants and the Phreesia client are missing from the complaint, but they may come to light as discovery proceeds on Phreesia's other claims.

IV. Conclusion

Defendants' motion to dismiss the CFAA claim and related conspiracy claim (Counts I and II) in their entirety is denied; however, due to the running of the CFAA statute of limitations, Phreesia may recover only for misconduct occurring on or after March 17, 2019. Defendants' motion to dismiss the tortious interference with a contractual relationship claim (Count IX) is granted. Count IX is dismissed without prejudice. Defendants must respond to the complaint within 21 days. Fed. R. Civ. P. 12(a)(4)(A).

All Citations

Slip Copy, 2022 WL 911207

Footnotes

[1] Phreesia filed its initial complaint on March 17, 2021. ECF 1. After defendants filed a Notice of Intent to File Motion to Dismiss Complaint, the Court held a case management conference on May 26 and allowed Phreesia to file an amended complaint to address the deficiencies defendants noted. ECF 25. Shortly after the conference, Phreesia filed an amended complaint. ECF 27.

[2] As is proper on a motion to dismiss, the Court takes all well-pleaded allegations contained in the amended complaint, ECF 27, as true. *Ray v. Roane*, 948 F.3d 222, 226 (4th Cir. 2020) (citing *King v. Rubenstein*, 825 F.3d 206, 212 (4th Cir. 2016)).

[3] Defendants also cite *Econ. Research Servs., Inc. v. Resolution Econ., LLC*, 208 F. Supp. 3d 219 (D.D.C. 2016), which concerned employees who accessed their employer's systems to acquire information and help a competitor. The Court dismissed the CFAA claim because all the alleged access was authorized. The case is not informative here; unlike the other cited cases, those who allegedly accessed the system were not third parties.

[4] This use of information and belief pleading is permissible. What defendants knew is within defendants' knowledge, and Phreesia alleges defendants operate in the same industry as competitors with similar products.

[5] Phreesia also alleges defendants deleted patient records as part of their use of the Phreesia System, ECF 27, ¶ 64, but it does not argue this constitutes “damage.” Phreesia's claim and arguments are focused entirely on the misappropriation of information. *See* ECF 33, at 12–13. Deleting patient records accessed through the system is not the same as deleting or modifying parts of the system's code. The deleted information was not a part of the system itself, but rather belonged to third parties.

[6] The parties discuss “damage” only in the context of the CFAA's statute of limitations, but the failure to allege “damage” has other implications for Phreesia's CFAA claim. The only provision Phreesia cited in its amended complaint, 18 U.S.C. § 1030(a)(5)(A), requires “damage” for a violation. Conversely, the provision cited by

defendants in their motion to dismiss, § 1030(a)(2)(C), does not. The latter provision is violated where the defendant "intentionally accesses a computer without authorization ... and thereby obtains information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). Phreesia does not allege damage, but its allegations do plausibly state a claim for a violation of § 1030(a)(2)(C). *See Estes Forwarding Worldwide LLC v. Cuellar*, 239 F. Supp. 3d 918, 922–23 (E.D. Va. 2017) (interpreting complaint that "unclear as to which specific provision of the CFAA it alleges [the defendant] violated" as alleging a violation of 18 U.S.C. § 1030(a)(2)(C), among other provisions, and denying motion to dismiss).

End of Document